Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

020.206 Certification and Accreditation

Version 2.2
March 8, 2018

Revision History

Date	Version	Description	Author
12/16/2011	1.0	Effective Date	CHFS IT Policies Team Charter
3/8/2018	2.2	Revision Date	CHFS OATS Policy Charter Team
3/8/2018	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	3/8/2018	Jennifer Harp	Jennifer Harp
CHFS Chief Security Officer (or designee)	3/8/2018	DENNIS E. LEBER	D. E

Table of Contents

Policy Definitions

- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

020.206 Certification and Accreditation

Category: 020.200 Managerial Security

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a certification and accreditation policy. This document establishes the agency’s Certification and Accreditation Policy to manage risks and provide guidelines for security best practices regarding the review and appropriate maintenance of the agency’s information system.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This positon is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) is designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This is role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

2.5 System Data Owner and System Data Administrators

It is the responsibility of these management/lead positons, to work with the application's development team to document components that are not included in the base server build and ensure backup are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

3 Policy Requirements

3.1 General Information

CHFS will certify and accredit any information systems, within OATS, that employs sensitive information, annually. Certification, accreditation, and security/risk assessments will be used to ensure appropriate levels of controls exist, they are managed, and are compliant with all federal and state laws and regulations. CHFS will ensure the most current baseline security requirements, as defined by the latest version of the National Institute of Standards and Technology (NIST) 800-53, are met.

3.2 Security Assessments

Per NIST 800-53, all application systems deemed critical by CHFS executive leadership, business partners, and other stakeholders, will at a minimum, annually undergo a partial or full security and privacy assessment. An assessment report will be generated with the results of the assessment. The assessment will be reviewed and approved by the appropriate system data owner and/or system data administrator and results will be shared with parties deemed appropriate.

3.3 Plan of Action and Milestones (POA&M)

Per NIST 800-53, all application systems deemed critical by CHFS executive leadership, business partners, and other stakeholders, will develop a Plan of Action and Milestones (POA&M). Findings and corrections, based on any audits, security impact analyses, monitoring activities or other review types, shall be documented and tracked in the Agency's POA&M. This will reduce or eliminate known vulnerabilities in the system.

The POA&M must be monitored and kept up to date on a regular basis. Please refer to the CHFS Plan of Action and Milestone(POA&M) Procedure established for agencies whom report to the Internal Revenue Service (IRS) or Centers for Medicare and Medicaid Services (CMS) for more actions.

3.4 Responsibility

The OATS IT Security and Compliance Team is responsible for oversight of vulnerability assessments of each system covered by this policy. If a third party is used, the OATS IT Security and Compliance Team is responsible to ensure that the vendor is a qualified organization as determined by COT.

3.5 Completion and Approval Process

The certification and accreditation process is performed by the OATS IS team. A senior level executive or manager will be appointed to authorize each agency's information system. Annually, the appointed executive or manager will validate the information system is approved before commencing operations.

This policy also aligns with all OATS and COT Enterprise policies pertaining to Data/Media Security.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 040.201 Internal Risk Assessment Policy
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Plan of Action and Milestone(POA&M) Procedure
- CHFS OATS Procedure: Risk Assessment Program Procedure

- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments Policy
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- National Institute of Standards and Technology (NIST) Special Publication 800-12 Revision 1, Introduction to Information Security (Draft)
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information